



THE EMERGING LAW OF ARTIFICIAL INTELLIGENCE IN AZERBAIJAN: Between National Strategy and European Regulatory Frameworks

Natig Khalilov 

Ph.D in Law, Independent Researcher, Azerbaijan

 nkhalilov@alu.ruc.edu.cn

ARTICLE INFO

Article History:

Received	18.08.2026
Accepted	27.08.2026
Published	30.09.2026

Keywords:

Artificial intelligence law,
Strategy-led modularism,
AI governance, Public-sector
AI, EU AI Act

ABSTRACT

Azerbaijan is moving from a general digital-development policy toward a distinct but still fragmented legal and institutional framework for artificial intelligence (AI). This article examines that transition through doctrinal legal research and functional comparative analysis. It evaluates constitutional and personal-data safeguards, the Artificial Intelligence Strategy for 2025–2028, national AI standards, digital-government infrastructure, regulatory experimentation, public-sector AI applications and the binding synthetic-media rules adopted in 2026. The article characterises the emerging model as strategy-led modularism: strategic direction, technical standards, institutional coordination and issue-specific legislation develop incrementally rather than through a single comprehensive AI statute. Comparison with the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law and the European Union Artificial Intelligence Act identifies the principal gap as the absence of enforceable lifecycle duties for high-impact systems, particularly where AI affects individual rights or structures the exercise of public authority. The article proposes a proportionate Azerbaijani Responsible AI Framework based on functional risk classification, impact assessment,

documentation, meaningful human oversight, public-sector procurement controls, incident reporting, effective remedies and institutionally credible supervision. It argues for regulatory interoperability with European and international models without mechanical institutional transplantation.

INTRODUCTION

Artificial-intelligence regulation increasingly requires states to reconcile innovation policy with legal certainty, rights protection and institutional accountability. International practice has not converged on one model: the European Union has adopted a detailed risk-based regulation, the Council of Europe has established treaty-level principles, while many states rely on combinations of strategy documents, sectoral law, standards and experimentation mechanisms.¹ The relevant legal question is therefore not simply whether a jurisdiction has enacted an “AI law”, but whether its institutions, binding rules and remedies govern consequential AI uses coherently.

Azerbaijan is an instructive case because its governance architecture changed rapidly in 2025–2026. The Artificial Intelligence Strategy for 2025–2028 made AI development a state priority and expressly anticipated a normative framework for responsible and ethical AI.² Its implementation plan requires normative legal acts on responsible AI and separate rules for identifying and preventing personal-data risks during system design, deployment and use.³

National standards, high-level digital coordination, regulatory pilots and targeted legislation have since added concrete elements to that strategic layer.

This article describes the resulting model as strategy-led modularism. The term denotes an incremental arrangement in which strategy, existing law, technical standards, public-sector infrastructure and issue-specific legislation co-exist before a comprehensive horizontal regime is established. Modularity can reduce transition costs and allow regulatory learning, but it also creates a risk that deployment will outpace enforceable safeguards. The central argument is that Azerbaijan need not replicate the institutional architecture of the EU AI Act; instead, it should establish a binding rights-based regulatory core for high-impact AI systems, particularly those used in public administration.⁴

The Azerbaijani legal literature on AI remains relatively limited and has largely addressed discrete questions rather than the emerging governance architecture as a whole. Vadiya Alakbarzade, a lecturer at the Faculty of Law of Baku State University, examines privacy, profiling, discrimination, transparency and legal accountability from a human-rights perspective.⁵ Shahla Samadova, Professor and Head of the Department of Criminal Law and Criminology at Baku State University, addresses criminal-law responsibility for AI-related harmful

1 Smuha, N. A. (2021). From a ‘race to AI’ to a ‘race to AI regulation’: Regulatory competition for artificial intelligence. *Law, Innovation and Technology*, 13(1), 57–84. <https://doi.org/10.1080/17579961.2021.1898300>.

2 Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028. (2025). Approved by Order of the President of the Republic of Azerbaijan of 19 March 2025. <https://president.az/az/articles/view/68365>.

3 Action Plan for the Implementation of the Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028. (2025). Actions 8.1.3 and 8.1.4.

4 Pavlidis, G. (2026). The EU AI Act and the Rights-Based Approach to Technological Governance. *Review of European and Comparative Law*, 64(1), 117–132. <https://doi.org/10.31743/recl.19283>.

5 Alakbarzade, V. (2025). Artificial intelligence in the context of international law: Human-rights and legal-accountability challenges. *Azerbaijan Law Journal*, 1.

conduct.⁶ These contributions provide important issue-specific foundations, but they do not fully integrate the institutional and legislative changes that matured during 2025–2026. The novelty of this article lies in analysing those developments as a connected governance model and testing their regulatory functions against the Council of Europe AI Framework Convention and the EU AI Act.

International scholarship has developed considerably since the EU AI Act was first proposed. Raposo's early doctrinal assessment identified risk classification, accountability and transparency as central points of tension in the European model.⁷ Laux, Wachter and Mittelstadt later argued that regulatory claims of "trustworthy AI" should not be reduced to a technical judgment that risks are acceptable, because trustworthiness also depends on institutional conditions and continuing accountability.⁸ Palmiotto's process-tracing analysis of the final Act further shows that the level of fundamental-rights protection reflects legislative compromise, making implementation, enforcement and judicial interpretation especially significant.⁹ These debates inform the present article's functional comparative method: European instruments are treated as sources of regulatory functions and safeguards, not as institutional templates for mechanical transplantation.

The research addresses three questions: how Azerbaijan has moved from general dig-

ital and data regulation toward AI-specific governance; how far the current framework operationalises rights-based and risk-based safeguards reflected in European instruments; and which regulatory functions can be adapted to Azerbaijan without mechanically transplanting foreign institutional structures. The analysis therefore considers whether Azerbaijan can preserve the flexibility of its modular approach while adding a binding rights-critical core for high-impact AI systems. The article first explains the methodology and legal context, then examines Azerbaijan's emerging governance model and principal regulatory gaps, compares the Council of Europe and EU benchmarks, and concludes with a proportionate national framework.

METHODOLOGY AND COMPARATIVE FRAMEWORK

The study combines doctrinal legal analysis with a functional comparative approach. The doctrinal analysis examines the relevant Azerbaijani legal and policy materials, including the Constitution, personal-data legislation, presidential instruments, AI and digital-development strategies, national standards, electronic-government rules and the 2026 synthetic-media reforms. The principal external benchmarks are the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law and the EU Artificial Intelligence Act. The comparison is functional rather than transplant-oriented: it evaluates which regulatory mechanisms—such as risk classification, impact assessment, documentation, human oversight, procurement controls, remedies and supervision—could be adapted to Azerbaijan's legal and administrative context. The doctrinal method is appropriate because the inquiry concerns the content, interaction and normative implications of constitutional, statutory and administrative instruments. The functional comparative approach is used because Azerbaijan is not an EU Member State; the relevant question is therefore which reg-

6 Samadova, Sh. T. (2025). Artificial intelligence and criminal law: Problems of responsibility. Baku University News: Social and Political Sciences Series.

7 Raposo, V. L. (2022). Ex machina: Preliminary critical assessment of the European Draft Act on artificial intelligence. *International Journal of Law and Information Technology*, 30(1), 88–109. <<https://doi.org/10.1093/ijlit/eaac007>>.

8 Laux, J., Wachter, S., Mittelstadt, B. (2024b). Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, 18(1), 3–32. <<https://doi.org/10.1111/rego.12512>>.

9 Palmiotto, F. (2025). The AI Act roller coaster: The evolution of fundamental rights protection in the legislative process and the future of the regulation. *European Journal of Risk Regulation*, 16(2), 770–793. <<https://doi.org/10.1017/err.2024.97>>.

ulatory functions, rather than which institutional forms, are transferable. Together, these methods enable the article to distinguish between the description of Azerbaijan's emerging regulatory framework and the normative recommendations advanced for its further development.

FINDINGS AND DISCUSSION

1. AZERBAIJAN'S EMERGING AI GOVERNANCE MODEL

1.1. Constitutional, data-protection and standards foundations

AI governance in Azerbaijan does not begin from a legal vacuum. Articles 24, 25 and 32 of the Constitution protect dignity, equality and private life and are directly relevant when algorithmic systems mediate public authority or process information about individuals.¹⁰ The Personal Data Law adds a more specific safeguard: Article 7.3 permits a person to object where a decision resulting from technologically mediated personal-data processing infringes the person's interests, subject to a statutory exception, while Articles 7.4 and 9 preserve complaint, compensation, purpose limitation, proportionality and data-quality requirements.¹¹

These provisions provide useful rights infrastructure but do not amount to a contemporary AI-accountability regime. They do not themselves establish a general duty to conduct AI-specific impact assessments, maintain life-cycle documentation, explain consequential outputs or provide structured human reconsideration.

At the international level, Azerbaijan is bound by Convention 108 on automated processing of personal data,¹² but it has not accepted the modernized Convention 108+ frame-

work.¹³ The future AI regime should therefore complement, rather than assume the completeness of, existing data-protection law.

Technical standards are another important layer. Azerbaijan adopted national standards derived from ISO/IEC instruments and in July 2025 adopted AZS ISO/IEC 42001:2025 on AI management systems.¹⁴ Standards can organise governance, testing and risk-management processes, but they cannot determine whether a public authority may lawfully deploy a system, what information an affected person must receive, or which remedy follows from unlawful use. Their proper role is evidentiary and operational: legislation should define rights and duties, while recognised standards provide reusable compliance methods.¹⁵ Recent scholarship on AI Act standardisation similarly warns that technical standards can embed contested normative choices about fairness, transparency and accountability unless public institutions retain responsibility for those judgments.¹⁶

1.2. Public administration, infrastructure and experimentation

The administrative dimension intensified in 2026. A presidential decree established the

10 Constitution of the Republic of Azerbaijan. (1995). Articles 24, 25 and 32.

11 Law of the Republic of Azerbaijan on Personal Data. (2010). Articles 7 and 9.

12 Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

13 Council of Europe Treaty Office. (n.d.). Chart of signatures and ratifications of Treaty 223: Protocol amending Convention 108—Azerbaijan entry. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyid=223>.

14 Azerbaijan Standardization Institute (AZSTAND). (July 28, 2025). New national standard adopted in the field of artificial intelligence: AZS ISO/IEC 42001:2025. <https://azstand.gov.az/az/xeberler/olkede-suni-intellekt-sahesinde-yeni-dovlet-standarti-qebul-edilib>.

15 International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. <https://www.iso.org/standard/42001>.

16 Laux, J., Wachter, S., Mittelstadt, B. (2024a). Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act. *Computer Law & Security Review*, 53, 105957. <https://doi.org/10.1016/j.clsr.2024.105957>.

Digital Development Council to coordinate digitalization, e-government, AI and innovation at a high political level.¹⁷ The Digital Development Acceleration Action Plan for 2026–2028 envisages broader public-sector AI, virtual assistants, high-performance computing and a legal framework for AI solutions successfully tested through a regulatory sandbox.¹⁸ This creates a strong implementation capacity, but coordination and promotion should remain conceptually distinct from independent legality and rights supervision.

The Electronic Government Information System (EGIS) consolidates authentication, consent, data exchange and digital public-service delivery across interoperable state subsystems.¹⁹ Such infrastructure can support AI-enabled administration at scale. Yet general requirements on data protection, information security and complaint rights do not answer AI-specific questions concerning impact assessment, model limitations, explanation, human review or post-deployment monitoring. Public-sector AI therefore requires an accountability layer connected directly to digital-government infrastructure.

A separate 2026 instrument created rules for regulatory pilot projects used to test digital solutions in state bodies.²⁰ Sandboxes can produce evidence before wider deployment, but they should not function as zones of di-

minished rights. High-impact public-sector pilots should have a defined legal basis, testing criteria, human-oversight arrangements, incident procedures and a transparent decision on whether the system may proceed to ordinary deployment. International guidance similarly treats regulatory sandboxes as supervised and time-limited mechanisms rather than general exemptions from law.²¹ Comparative analysis of the AI Act's sandbox regime likewise shows that experimentation can support innovation, but only if legality, equality, liability and participant safeguards remain explicit constraints on testing.²²

Public legal-information systems illustrate the practical stakes. The E-qanun.ai platform, officially presented in September 2025, combines legal databases with AI-assisted search and analysis.²³ Research on specialised AI legal-research tools shows that retrieval-based systems may still generate inaccurate or unsupported legal information.²⁴ Public legal AI should therefore preserve direct access to authoritative sources, distinguish official text from generated analysis, document system versions and limitations, and evaluate performance specifically in Azerbaijani legal language.

17 Decree on certain measures to improve activities in the fields of digitalization, e-government, artificial intelligence and innovation in the Republic of Azerbaijan. (February 27, 2026). <https://president.az/ru/articles/view/71718>.

18 President of the Republic of Azerbaijan. (February 27, 2026). Action Plan for the Acceleration of Digital Development in the Republic of Azerbaijan for 2026–2028. <https://president.az/az/articles/view/71720>.

19 Regulation on the Electronic Government Information System. (August 12, 2025). Approved by Decree No. 472 of the President of the Republic of Azerbaijan. <https://e-qanun.az/framework/60355>.

20 Rules for the implementation of regulatory pilot projects for test-mode evaluation of digital solutions applied by state bodies and for determining the initial feasibility of electronic services organised by state bodies. (April 30, 2026). <https://president.az/az/articles/view/72251>.

21 Organisation for Economic Co-operation and Development. (2023). Regulatory sandboxes in artificial intelligence (OECD Digital Economy Papers No. 356). OECD Publishing.

22 Buocz, T., Pfothenhauer, S., Eisenberger, I. (2023). Regulatory sandboxes in the AI Act: Reconciling innovation and safety? *Law, Innovation and Technology*, 15(2), 357–389. <https://doi.org/10.1080/17579961.2023.2245678>.

23 Ministry of Digital Development and Transport of the Republic of Azerbaijan. (September 25, 2025). E-qanun.ai platform officially presented. <https://mincom.gov.az/en/media-en/news/e-qanunai-platform-officially-presented>.

24 Magesh, V., Surani, F., Dahl, M., Suzgun, M., Manning, C. D., Ho, D. E. (2025). Hallucination-free? Assessing the reliability of leading AI legal research tools. *Journal of Empirical Legal Studies*, 22(2), 216–242. <https://doi.org/10.1111/jels.12413>.

1.3. The 2026 synthetic-media reforms

The clearest move from policy to AI-specific hard law occurred in April 2026, when Azerbaijan amended criminal, procedural, information and media legislation. The reforms introduced criminal liability for specified non-consensual AI-enabled uses of a person's image or voice, including a separate offence concerning pornographic or sexual synthetic material. They also introduced disclosure duties for publicly displayed AI-generated photo, video or audio material and administrative liability for knowing dissemination without the required label.²⁵

The reforms are important because they show that Azerbaijan is already regulating AI through a modular combination of criminal, administrative, media and information law. Their limits are equally instructive. A future horizontal framework should supply common, technology-neutral definitions and coordinated principles for liability, transparency and enforcement. It should also clarify the treatment of legitimate journalism, satire, art, research and security testing without weakening protection against malicious impersonation or non-consensual sexual synthetic content.

2. THE PRINCIPAL REGULATORY GAPS

2.1. High-impact systems and lifecycle accountability

The principal gap is the absence of a binding cross-sectoral regime for systems that materially affect rights, essential services, significant opportunities or the exercise of public power. A high-impact category should therefore be defined functionally: it should cover systems that determine, recommend, rank, predict or sub-

stantially influence consequential decisions in fields such as public benefits, employment, education, credit, healthcare, policing, migration, biometric identification and the administration of justice. Systems that allocate public resources or determine inspection and enforcement priorities may also warrant this classification when their outputs structure public authority.

Lifecycle regulation is necessary because AI risk is socio-technical. Harm may arise from objectives, data selection, proxy variables, performance thresholds, deployment context, human-machine interaction or later system updates. Accountability must accordingly extend from design and procurement through deployment, monitoring, modification and retirement. End-to-end auditing scholarship similarly emphasises allocation of responsibility across development and organisational use rather than relying only on retrospective investigation after harm occurs.²⁶ Jonas Schuett, Senior Research Fellow at the Centre for the Governance of AI, analyses the AI Act's risk-management duty as a continuous process extending beyond initial classification and pre-deployment testing.²⁷ Gianclaudio Malgieri, Associate Professor of Law and Technology at the eLaw Center for Law and Digital Technologies at Leiden University, and Frank Pasquale, Professor of Law at Cornell Tech and Cornell Law School, likewise argue that high-risk AI may warrant ex ante justification rather than reliance solely on ex post liability.²⁸ Martin Ebers, Visiting Professor of Information

25 Law of the Republic of Azerbaijan on amendments to the Criminal Code, the Code of Criminal Procedure, the Law on Information, Informatization and Protection of Information, and the Law on Media. (April 21, 2026). <https://president.az/az/articles/view/72311>.

26 Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 33–44). Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372873>.

27 Schuett, J. (2024). Risk management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, 15(2), 367–385. <https://doi.org/10.1017/err.2023.1>.

28 Malgieri, G., Pasquale, F. (2024). Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology. *Computer Law & Security Review*, 52, 105899. <https://doi.org/10.1016/j.clsr.2023.105899>.

Technology Law at the University of Tartu, further argues that implementation of the AI Act should follow a genuinely risk-based approach, with regulatory obligations calibrated to the nature and intensity of the risks involved.²⁹

Providers should be responsible for design, testing, technical documentation, known limitations and material updates. Deployers should be responsible for lawful purpose, contextual suitability, operational monitoring and competent human oversight. Public authorities should remain legally responsible for decisions taken in their name even when the system is procured or accessed as a service from a private supplier. Outsourcing technology must not outsource constitutional or administrative accountability.

2.2. From objection to effective contestability

The Personal Data Law's right to object is a useful starting point but does not expressly guarantee AI-specific notice, case-specific reasons or meaningful human reconsideration. For a high-impact decision, the affected person should be told that AI materially contributed to the outcome, receive understandable information about the system's role and the principal factors relevant to the case, and have access to a reviewer with authority to disregard or reverse the system's output. Contestability does not require disclosure of source code; it requires enough information to identify possible errors and exercise legal rights. Guillermo Lazcoz, a legal researcher at the Spanish Biomedical Research Centre on Rare Diseases (CIBERER), and Paul De Hert, Professor of Law at Vrije Universiteit Brussel and Associate Professor at Tilburg University, treat human intervention as part of a broader accountability system rather than a formal checkpoint that can be satis-

fied merely by placing a person "in the loop".³⁰ Non-discrimination safeguards also require context-sensitive legal analysis, because statistical fairness metrics cannot automatically reproduce the substantive and evidentiary tests used in EU equality law.³¹

Impact assessment should also extend beyond conventional data protection. An AI or fundamental-rights assessment should examine purpose, necessity, proportionality, affected groups, error distribution, discrimination, institutional context and less intrusive alternatives. This broader model reflects scholarship calling for integrated human-rights, social and ethical assessment of AI and data-intensive systems.³² Recent work on fundamental-rights impact assessment under the AI Act demonstrates how rights analysis can be operationalised through structured contextual information, identification of affected rights and traceable evaluation criteria.³³

2.3. Procurement and institutional accountability

Public procurement is a central regulatory lever because public authorities may depend on external suppliers for AI models, software

29 Ebers, M. (2025). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation*, 16(2), 684–703. <https://doi.org/10.1017/err.2024.78>.

30 Lazcoz, G., De Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems: Essential pre-requisites against abdicating responsibilities. *Computer Law & Security Review*, 50, 105833. <https://doi.org/10.1016/j.clsr.2023.105833>.

31 Wachter, S., Mittelstadt, B., Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567. <https://doi.org/10.1016/j.clsr.2021.105567>.

32 Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 34(4), 754–772. <https://doi.org/10.1016/j.clsr.2018.05.017>.

33 Bertaina, S., Biganzoli, I., Desiante, R., Fontanella, D., Inverardi, N., Penco, I. G., Cosentini, A. (2025). Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of AI Act. *Computer Law & Security Review*, 56, 106101. <https://doi.org/10.1016/j.clsr.2024.106101>.

and cloud services. Azerbaijan's Law on Public Procurement provides a partial legal basis for incorporating AI-related safeguards into procurement procedures. Article 22 permits procurement specifications to include technical, quality, performance and testing requirements, while Article 23 allows suppliers' professional and technical capacity to be assessed. Tender documentation must also contain detailed technical requirements and the draft procurement contract.³⁴ These provisions give contracting authorities some scope to require documentation, testing, cybersecurity safeguards and supplier capabilities relevant to high-impact AI systems. The existing framework nevertheless contains important deficiencies when applied to AI. It does not expressly require fundamental-rights impact assessment, algorithmic auditability, human-oversight arrangements, lifecycle logging, notification of material model changes or serious-incident reporting. Moreover, Article 33.11 limits the assessment of the "most efficient offer" to operating, maintenance and repair costs, delivery or performance periods, functional characteristics and warranty conditions, while Article 33.12 requires the relevant criteria to be quantitatively assessable or capable of being expressed in value terms. This approach may underweight characteristics such as transparency, auditability, data governance and rights protection that are especially important when public authorities procure high-impact AI. Article 42 also generally restricts modification of contractual terms after the procurement contract has entered into force.³⁵ AI-specific safeguards should therefore be incorporated *ex ante*, including requirements concerning documentation, audit access, log retention, cybersecurity, model-change notification, incident reporting, data portability and supplier cooperation with supervisory authorities.

34 Law of the Republic of Azerbaijan on Public Procurement, No. 988-VIQ of 14 July 2023, Articles 22, 23 and 25.

35 Law of the Republic of Azerbaijan on Public Procurement, Articles 33.11–33.12 and 42.

The EU AI Act provides a useful comparative benchmark because accountability does not end with acquisition of the system. Article 26 imposes continuing obligations on deployers of high-risk AI systems concerning human oversight, monitoring, risk notification, serious incidents and cooperation with competent authorities; public-authority deployers are additionally subject to registration requirements. Article 27 requires specified public bodies and providers of public services to conduct a fundamental-rights impact assessment before deploying certain high-risk systems.³⁶ The relevant lesson for Azerbaijan is therefore not to reproduce the EU regulatory architecture, but to connect procurement requirements with continuing public-law obligations throughout deployment. A public authority should remain legally responsible for an AI-enabled administrative function even where the underlying technology is supplied by a private contractor.

From an administrative-law perspective, Oriol Mir, Full Professor of Administrative Law at Pompeu Fabra University, similarly examines the impact of the EU AI Act on public authorities when they develop, acquire and use AI systems. He argues that, despite certain limitations, the Act represents an important step towards addressing established problems associated with automated administrative decision-making and public-sector AI.³⁷

A public-sector AI register would complement these safeguards in Azerbaijan by identifying, for each high-impact system, the responsible authority, supplier where applicable, intended purpose and legal basis, deployment date, human-oversight arrangements and a summary of the relevant impact assessment. Legitimate confidentiality exceptions may be

36 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). Official Journal of the European Union, L 2024/1689. Articles 26, 27 and 49.

37 Mir, O. (2025). The AI Act from the perspective of administrative law: Much ado about nothing? *European Journal of Risk Regulation*, 16(1), 63–75. <https://doi.org/10.1017/err.2024.54>.

necessary, but non-disclosure should require justification rather than operate as the default.

3. COMPARATIVE BENCHMARKS

3.1. Council of Europe Framework Convention

The Council of Europe AI Framework Convention could be a particularly suitable benchmark because it is organised around human rights, democracy and the rule of law rather than a specific internal-market architecture. It requires principles of dignity, autonomy, equality, transparency, accountability, privacy and reliability to be supported by remedies, procedural safeguards and iterative risk-management measures throughout the AI lifecycle.³⁸ The Convention also requires oversight mechanisms to act independently and impartially and to possess appropriate powers and expertise. Vladislava Stoyanova, Associate Professor of Public International Law at the Faculty of Law of Lund University, argues that the Convention does not create a separate catalogue of AI-specific human rights; rather, it requires states to operationalise existing human-rights obligations across AI lifecycles through context-sensitive measures.³⁹

To date, Azerbaijan has not signed the Council of Europe AI Framework Convention.⁴⁰ Nevertheless, the Convention could serve as a useful outcome-based benchmark for the de-

velopment of domestic AI regulation. Its relevance lies less in institutional replication than in the regulatory questions it requires states to address: whether individuals can identify and challenge AI-supported decisions, whether risk assessments adequately consider fundamental rights and democratic institutions, whether public authorities remain accountable when AI systems are supplied or operated by private actors, and whether supervisory mechanisms are sufficiently independent and effective. These considerations are compatible with Azerbaijan's emerging modular approach and could inform the development of domestic safeguards without requiring the transplantation of institutional structures designed for the EU internal market.

3.2. EU Artificial Intelligence Act

The EU AI Act offers a more detailed comparator. It allocates duties among providers and deployers, regulates specified high-risk systems, establishes obligations concerning documentation, logging, transparency, human oversight, robustness and post-market monitoring, and creates separate rules for general-purpose AI. Particularly relevant to Azerbaijan are the fundamental-rights impact assessment for specified deployers, transparency duties for synthetic content, regulatory sandboxes and the right of certain affected persons to obtain explanations concerning consequential high-risk decisions.⁴¹

The July 2026 amendments postponed the application of key requirements for high-risk AI systems, principally to December 2027 for systems listed in Annex III and August 2028 for systems linked to the product-safety legislation listed in Annex I.⁴² The amendment expressly re-

38 Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), especially Articles 3, 8–14 and 26.

39 Stoyanova, V. (2026). Council of Europe Framework Convention on Artificial Intelligence: Context, regulatory approach and scope of obligations. *European Journal of Risk Regulation*, 17(2), 536–565. <https://doi.org/10.1017/err.2025.10070>.

40 Council of Europe Treaty Office. (n.d.). Chart of signatures and ratifications of Treaty 225: Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law—Azerbaijan entry. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyid=225>.

41 Regulation (EU) 2024/1689, Arts. 13, 26, 27, 50, 51–57, 72–73 and 86.

42 Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards simplification of the im-

flects concerns about the delayed availability of standards, guidance and institutional capacity. This experience illustrates a broader regulatory lesson for Azerbaijan: substantive obligations are unlikely to operate effectively unless standards, testing capacity, complaint mechanisms and supervisory expertise are developed alongside them. Azerbaijan should therefore borrow regulatory functions rather than legislative volume and phase demanding obligations in parallel with the institutions required to implement and enforce them.

The EU model may also have practical relevance for Azerbaijani businesses because the EU AI Act can reach providers outside the Union when they place systems or general-purpose models on the EU market or when system output is used within the Union.⁴³ Greater regulatory interoperability in terminology, documentation, testing and incident reporting could therefore facilitate cross-border compliance and reduce regulatory fragmentation for firms operating across markets, while domestic law remains tailored to Azerbaijan's constitutional and administrative structure.⁴⁴

Taken together, the two European benchmarks perform complementary functions for the Azerbaijani context. The Council of Europe Convention supplies an outcome-oriented framework centred on human rights, democratic safeguards and institutional accountability, whereas the EU AI Act provides more detailed operational mechanisms for translating comparable concerns into lifecycle obligations for particular actors and categories of AI systems. Azerbaijan could therefore draw on the Convention for the normative core of its emerging framework while selectively adapting operational mechanisms from the EU AI Act where

they correspond to domestic regulatory needs and institutional capacity.

4. A PROPORTIONATE RESPONSIBLE AI FRAMEWORK FOR AZERBAIJAN

The Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028 already provides a political mandate for responsible-AI legislation. In the author's view, a proportionate regulatory framework may translate that mandate into enforceable rules through five connected elements.

First, legislation should define AI systems and relevant actors in technologically durable terms and allocate responsibility according to actual control over risk.

Second, it should establish functional risk tiers, including narrowly defined prohibited practices and a high-impact category based on material effects rather than the supplier's label.

Third, every high-impact system should be subject to a documented lifecycle process. Before deployment, the responsible entity should establish the lawful purpose, affected groups, data sources, foreseeable misuse, performance limits and rights impacts. Testing should address accuracy, robustness, discriminatory performance, cybersecurity and suitability for Azerbaijani linguistic and institutional conditions. During operation, systems should produce proportionate logs, preserve material-change records and support competent human intervention. Serious incidents and complaints should trigger investigation, correction, suspension or retirement where necessary.

Fourth, public-sector use should attract heightened duties because government combines data access, scale and coercive or allocative authority. A public authority deploying high-impact AI should complete an impact assessment, publish registry information, apply standardised procurement clauses and preserve meaningful human review. These functions parallel safeguards found in the EU AI Act,

plementation of harmonised rules on artificial intelligence. (2026). Official Journal of the European Union, L 2026/1744.

43 Regulation (EU) 2024/1689. Article 2.

44 Gonzalez Torres, A. P., Ali-Vehmas, T. (2025). AI regulation: Maintaining interoperability through value-sensitive standardisation. *Ethics and Information Technology*, 27, 26. <https://doi.org/10.1007/s10676-025-09832-7>.

including impact assessment and explanation rights,⁴⁵ while remaining adaptable to Azerbaijani administrative procedure.

Fifth, supervision should be institutionally credible. Strategic coordination may remain with bodies responsible for digital development, but complaint handling, legality review and enforcement should be assigned to an authority or coordinated set of authorities with sufficient independence, expertise, investigatory powers and resources. This separation between promotion and supervision is consistent with the institutional logic of the Council of Europe Convention.⁴⁶ Remedies should include correction of unlawful processing or decisions, human reconsideration, suspension of unsafe systems and access to judicial or administrative review.

General-purpose AI requires a related but distinct layer. Model providers should disclose capabilities, known limitations, cybersecurity measures and material updates sufficient for downstream deployers to comply with their own duties. Enhanced obligations should apply only where scale, capabilities or demonstrated risks justify them. Azerbaijani-language public-service and legal systems should be evaluated on representative local-language data and tested for retrieval and citation accuracy rather than assumed reliable because of performance on English benchmarks.

Synthetic-content rules should likewise be supported by technical guidance on human-readable labels and, where feasible, machine-readable provenance. Open provenance standards can assist in recording origin and modification history, but they do not prove factual truth and cannot replace consent requirements, platform responsibility or remedies for harmful content.⁴⁷

Implementation should be phased. Immediate measures should include an inventory of

public-sector AI, interim impact assessments for high-impact procurements and pilots, standard contractual clauses, guidance for synthetic-media disclosure and documented evaluation requirements for public-facing AI assistants. The existing Digital Development Acceleration Action Plan makes these safeguards urgent because it already anticipates wider AI-enabled public services and regulatory experimentation. The next phase should enact the horizontal framework and operationalise supervision, incident reporting, complaint procedures and coordinated sectoral rules. A later statutory review should assess regulatory costs, complaint and incident patterns, innovation effects, supervisory capacity and the continuing suitability of risk categories.

CONCLUSION

Azerbaijan has moved beyond an AI policy consisting only of strategic aspirations. Constitutional and personal-data rules, national standards, digital-government infrastructure, regulatory pilots, institutional coordination and the 2026 synthetic-media legislation now form an emerging legal architecture. Its defining feature is strategy-led modularism: binding and non-binding elements are being assembled incrementally rather than through a single comprehensive statute.

The model is flexible but incomplete. The principal deficiency is not the absence of ethical principles; it is the absence of enforceable lifecycle obligations for high-impact systems and a corresponding structure for contestability, public-sector procurement, incident handling and independent supervision. Those gaps are especially important where AI materially affects individual rights, access to public services or the exercise of public authority.

Azerbaijan should therefore adopt a proportionate responsible-AI framework that preserves the advantages of modular development while adding a binding rights-critical core. International and European instruments should

45 Regulation (EU) 2024/1689. Articles 27 and 86.

46 Council of Europe AI Framework Convention (CETS No. 225), Articles 9–14 and 26.

47 Coalition for Content Provenance and Authenticity. (April, 2026). C2PA technical specification (Version 2.4). <https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html>.

be used as functional benchmarks: impact assessment, documentation, meaningful human oversight, remedies and credible supervision are transferable regulatory functions, while institutional structures specific to the EU internal market need not be copied. This approach would allow Azerbaijan to pursue regulatory interoperability without regulatory dependency

and to align AI-enabled public administration with legal accountability.

Future research should assess how these safeguards operate in practice as Azerbaijan implements the 2025–2028 AI Strategy, particularly in public-sector deployments and in the development of any subsequent horizontal AI legislation.

REFERENCES:

Scholarly Literature:

- Alakbarzade, V. (2025). Artificial intelligence in the context of international law: Human-rights and legal-accountability challenges. *Azerbaijan Law Journal*, 1. (in Azerbaijani);
- Bertaina, S., Biganzoli, I., Desiante, R., Fontanella, D., Inverardi, N., Penco, I. G., Cosentini, A. (2025). Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of AI Act. *Computer Law & Security Review*, 56, 106101. <https://doi.org/10.1016/j.clsr.2024.106101>;
- Buocz, T., Pfothenauer, S., Eisenberger, I. (2023). Regulatory sandboxes in the AI Act: Reconciling innovation and safety? *Law, Innovation and Technology*, 15(2). <https://doi.org/10.1080/17579961.2023.2245678>;
- Ebers, M. (2025). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation*, 16(2). <https://doi.org/10.1017/err.2024.78>;
- Gonzalez Torres, A. P., Ali-Vehmas, T. (2025). AI regulation: Maintaining interoperability through value-sensitive standardisation. *Ethics and Information Technology*, 27. <https://doi.org/10.1007/s10676-025-09832-7>;
- Laux, J., Wachter, S., Mittelstadt, B. (2024a). Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act. *Computer Law & Security Review*, 53. <https://doi.org/10.1016/j.clsr.2024.105957>;
- Laux, J., Wachter, S., Mittelstadt, B. (2024b). Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, 18(1). <https://doi.org/10.1111/reg.12512>;
- Lazcoz, G., De Hert, P. (2023). Humans in the GDPR and AIA governance of automated and algorithmic systems: Essential pre-requisites against abdicating responsibilities. *Computer Law & Security Review*, 50, 105833. <https://doi.org/10.1016/j.clsr.2023.105833>;
- Magesh, V., Surani, F., Dahl, M., Suzgun, M., Manning, C. D., Ho, D. E. (2025). Hallucination-free? Assessing the reliability of leading AI legal research tools. *Journal of Empirical Legal Studies*, 22(2). <https://doi.org/10.1111/jels.12413>;
- Malgieri, G., Pasquale, F. (2024). Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology. *Computer Law & Security Review*, 52, 105899. <https://doi.org/10.1016/j.clsr.2023.105899>;
- Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer*

- Law & Security Review, 34(4). <https://doi.org/10.1016/j.clsr.2018.05.017>;
- Mir, O. (2025). The AI Act from the perspective of administrative law: Much ado about nothing? *European Journal of Risk Regulation*, 16(1). <https://doi.org/10.1017/err.2024.54>;
- Palmiotto, F. (2025). The AI Act roller coaster: The evolution of fundamental rights protection in the legislative process and the future of the regulation. *European Journal of Risk Regulation*, 16(2). <https://doi.org/10.1017/err.2024.97>;
- Pavlidis, G. (2026). The EU AI Act and the Rights-Based Approach to Technological Governance. *Review of European and Comparative Law*, 64(1). <https://doi.org/10.31743/recl.19283>;
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372873>;
- Raposo, V. L. (2022). Ex machina: Preliminary critical assessment of the European Draft Act on artificial intelligence. *International Journal of Law and Information Technology*, 30(1). <https://doi.org/10.1093/ijlit/eaac007>;
- Samadova, Sh. T. (2025). Artificial intelligence and criminal law: Problems of responsibility. *Baku University News: Social and Political Sciences Series*. (in Azerbaijani);
- Schuett, J. (2024). Risk management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, 15(2). <https://doi.org/10.1017/err.2023.1>;
- Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. *Law, Innovation and Technology*, 13(1). <https://doi.org/10.1080/17579961.2021.1898300>;
- Stoyanova, V. (2026). Council of Europe Framework Convention on Artificial Intelligence: Context, regulatory approach and scope of obligations. *European Journal of Risk Regulation*, 17(2). <https://doi.org/10.1017/err.2025.10070>;
- Wachter, S., Mittelstadt, B., Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567. <https://doi.org/10.1016/j.clsr.2021.105567>.

Normative Acts:

- Action Plan for the Implementation of the Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028. (2025). Actions 8.1.3 and 8.1.4. (in Azerbaijani);
- Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028. (2025). Approved by Order of the President of the Republic of Azerbaijan of 19 March 2025. <https://president.az/az/articles/view/68365>. (in Azerbaijani);
- Constitution of the Republic of Azerbaijan. (1995). (in Azerbaijani);
- Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);
- Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225);
- Decree on certain measures to improve activities in the fields of digitalization, e-government, artificial intelligence and innovation in the Republic of Azerbaijan. (February 27, 2026). <https://president.az/ru/articles/view/71718>. (in Russian);
- Law of the Republic of Azerbaijan on amendments to the Criminal Code, the Code of

- Criminal Procedure, the Law on Information, Informatization and Protection of Information, and the Law on Media. (April 21, 2026). <https://president.az/az/articles/view/72311>. (in Azerbaijani);
- Law of the Republic of Azerbaijan on Personal Data. (2010). (in Azerbaijani);
- Law of the Republic of Azerbaijan on Public Procurement, No. 988-VIQ of 14 July 2023. (in Azerbaijani);
- President of the Republic of Azerbaijan. (February 27, 2026). Action Plan for the Acceleration of Digital Development in the Republic of Azerbaijan for 2026–2028. <https://president.az/az/articles/view/71720>. (in Azerbaijani);
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). Official Journal of the European Union, L 2024/1689;
- Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards simplification of the implementation of harmonised rules on artificial intelligence. (2026). Official Journal of the European Union, L 2026/1744;
- Regulation on the Electronic Government Information System. (August 12, 2025). Approved by Decree No. 472 of the President of the Republic of Azerbaijan. <https://e-qanun.az/framework/60355>. (in Azerbaijani);
- Rules for the implementation of regulatory pilot projects for test-mode evaluation of digital solutions applied by state bodies and for determining the initial feasibility of electronic services organised by state bodies. (April 30, 2026). <https://president.az/az/articles/view/72251>. (in Azerbaijani).
- al standard adopted in the field of artificial intelligence: AZS ISO/IEC 42001:2025. <https://azstand.gov.az/az/xeberler/olkede-suni-intellekt-sahesinde-yeni-dovlet-standardi-qebul-edilib>. (in Azerbaijani);
- Coalition for Content Provenance and Authenticity. (April, 2026). C2PA technical specification (Version 2.4). https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html;
- Council of Europe Treaty Office. (n.d.). Chart of signatures and ratifications of Treaty 223: Protocol amending Convention 108—Azerbaijan entry. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=223>;
- Council of Europe Treaty Office. (n.d.). Chart of signatures and ratifications of Treaty 225: Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law—Azerbaijan entry. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=225>;
- International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system. <https://www.iso.org/standard/42001>;
- Ministry of Digital Development and Transport of the Republic of Azerbaijan. (September 25, 2025). E-qanun.ai platform officially presented. <https://mincom.gov.az/en/media-en/news/e-qanunai-platform-officially-presented>;
- Organisation for Economic Co-operation and Development. (2023). Regulatory sandboxes in artificial intelligence (OECD Digital Economy Papers No. 356). OECD Publishing.

Other Supplementary Materials:

Azerbaijan Standardization Institute (AZ-
STAND). (July 28, 2025). New nation-